대한민국특허청
KOREAN INTELLECTUAL PROPERTY OFFICE

별첨 사본은 아래 출원의 원본과 동일함을 증명함.

This is to certify that the following application annexed hereto is a true copy from the records of the Korean Intellectual Property Office.

출 원 번 호 : 10-2003-0067442
Application Number

출 원 년 월 일 : 2003년 09월 29일
Date of Application SEP 29, 2003

출 원 인 : 한국전자통신연구원
Applicant(s) Electronics and Telecommunications Research Inst

2003 년 11 월 13 일

특 허 청
COMMISSIONER

【서지사항】

【서류명】	특허출원서
【권리구분】	특허
【수신처】	특허청장
【참조번호】	0001
【제출일자】	2003.09.29
【발명의 명칭】	네트워크 노드의 보안 엔진 관리 장치 및 방법
【발명의 영문명칭】	SECURITY ENGINE MANAGEMENT APPARATUS AND METHOD IN NETWORK NODES
【출원인】	
【명칭】	한국전자통신연구원
【출원인코드】	3-1998-007763-8
【대리인】	
【성명】	장성구
【대리인코드】	9-1998-000514-8
【포괄위임등록번호】	2001-038646-2
【대리인】	
【성명】	김원준
【대리인코드】	9-1998-000104-8
【포괄위임등록번호】	2001-038648-7
【발명자】	
【성명의 국문표기】	조수형
【성명의 영문표기】	JO,Su Hyung
【주민등록번호】	740119-2709729
【우편번호】	305-728
【주소】	대전광역시 유성구 전민동 세종아파트 105-1108
【국적】	KR
【발명자】	
【성명의 국문표기】	김정녀
【성명의 영문표기】	KIM,Jeong Nyeo
【주민등록번호】	650919-2565712
【우편번호】	302-727
【주소】	대전광역시 서구 내동 코오롱아파트 8-801
【국적】	KR

【발명자】

【성명의 국문표기】 손승원

【성명의 영문표기】 SOHN,Sung Won

【주민등록번호】 571225-1674514

【우편번호】 305-761

【주소】 대전광역시 유성구 전민동 엑스포아파트 208-902

【국적】 KR

【공지예외적용대상증명서류의 내용】

【공개형태】 학술단체 서면발표

【공개일자】 2003.05.16

【공지예외적용대상증명서류의 내용】

【공개형태】 학술단체 서면발표

【공개일자】 2003.06.23

【심사청구】 청구

【취지】 특허법 제42조의 규정에 의한 출원, 특허법 제60조의 규정에 의한 출원심사 를 청구합니다. 대리인
장성구 (인) 대리인
김원준 (인)

【수수료】

【기본출원료】	20	면	29,000 원
【가산출원료】	6	면	6,000 원
【우선권주장료】	0	건	0 원
【심사청구료】	15	항	589,000 원

【합계】 624,000 원

【감면사유】 정부출연연구기관

【감면후 수수료】 312,000 원

【기술이전】

【기술양도】 희망

【실시권 허여】 희망

【기술지도】 희망

【첨부서류】 1. 요약서·명세서(도면)_1통 2.공지예외적용대상(신규성상실의예외, 출원시의특례)규정을 적용받 기 위한 증명서류_2통

【요약서】

【요약】

본 발명은 네트워크 노드의 보안 엔진 관리 장치 및 방법에 관한 것으로, 시스템의 자원에 접근할 수 있는 모든 응용 프로그램과 유틸리티들을 처리하는 보안 명령어 및 라이브러리 서브시스템과, 네트워크로의 침입 탐지 및 차단에 필요한 필터링 정책, 침입 탐지 정책, 접근 제어 정책을 결정하는 정책 결정 서브시스템과, 접근 제어 정책을 참조하여 허가받지 않은 사용자의 시스템 사용을 막고 모든 주체는 객체에 접근 할 수 있는 권한을 가진 경우에만 접근이 가능하도록 하는 인증 및 접근제어 서브시스템과, 정책들을 해석하여 정책을 적용하는 정책 적용 서브시스템과, 정책 적용에 따라 필터링 정책을 참조하면서 허가된 패킷은 수신하고, 허가되지 않은 패킷을 거부하는 패킷 필터링 서브시스템과, 정책 적용에 따라 침입탐지 정책을 참조하면서 네트워크의 침입을 분석하고 침입에 대응하는 침입 분석 및 감사 추적 서브시스템과, 보안 엔진을 관리하는 보안 관리 서브시스템을 포함한다. 네트워크 노드를 보안 정책에 의해 관리하여 보안 환경의 변화에 민첩하게 대처할 수 있다. 또한, 기존 네트워크 노드들의 자체 보안 결함을 해결하며 통합적인 보안 관리를 제공하고, 웹 브라우저를 사용하여 관리의 편리성과 효율성을 제공하는 효과가 있다.

【대표도】

도 2

【명세서】

【발명의 명칭】

네트워크 노드의 보안 엔진 관리 장치 및 방법{SECURITY ENGINE MANAGEMENT APPARATUS AND METHOD IN NETWORK NODES}

【도면의 간단한 설명】

도 1은 본 발명의 바람직한 실시 예에 따른 공격 시스템으로부터 침입을 차단하는 보안 엔진의 개괄적인 구성도를 도시한 도면이고,

도 2는 도 1에 도시된 보안 엔진의 상세 구성도이며,

도 3은 도 2에 도시된 보안 관리 서브시스템의 상세 구성도이며,

도 4는 본 발명에 따른 공격 시스템의 침입을 탐지하고 실시간으로 대응하는 보안 엔진의 동작 과정에 대한 상세 흐름도이며,

도 5는 본 발명에 따른 보안 엔진이 탑재된 라우터와 보안 관리 서브시스템간의 보안 정책에 의해 통합적으로 보안 관리를 제공하는 과정에 대한 상세 흐름도이다.

<도면의 주요부분에 대한 부호의 설명>

100 : 보안 엔진이 탑재된 라우터

110 : 보안 명령어 및 라이브러리 서브시스템

120-1 : 정책 데이터베이스 120 : 정책 결정 서브시스템

130-1 : 접근 제어 정책 130 : 인증 및 접근제어 서브시스템

140 : 정책 적용 서브시스템 150-1 : 필터링 정책

150 : 패킷 필터링 서브시스템 160-2 : 침입 탐지 정책

160-1 : 감사 기록 데이터베이스

160 : 침입 분석 및 감사 추적 서브시스템

200 : 보안 관리 서브시스템 201 : 로그인 처리 모듈

202 : 패킷 통계 모듈 203 : 네트워크 설정 모듈

204 : 정책 관리 모듈 205 : 감사 관리 모듈

206 : XML Java Bean 207 : 사용자 데이터베이스

208 : 네트워크 데이터베이스 209 : 네트워크 통신 모듈

【발명의 상세한 설명】

【발명의 목적】

【발명이 속하는 기술분야 및 그 분야의 종래기술】

<20> 본 발명은 네트워크 노드의 보안 엔진 관리 장치 및 방법에 관한 것으로, 특히 네트워크 노드의 보안을 위해 커널 영역에서 패킷 필터링, 인증 및 접근제어 관리, 침입 분석 및 감사 추적을 제공하며, 보안 정책에 의한 보안 엔진을 관리하도록 하는 장치 및 방법에 관한 것이다.

<21> 일반적으로, 인터넷의 급속한 발전과 보급으로 네트워크 환경은 점점 거대해지고 있으며, 인터넷의 간편하고 편리한 네트워크 접속과 제공하고 있는 다양한 서비스로 인하여 그 형태가 복잡해지고 있다.

<22> 그러나, 인터넷 상에서의 바이러스, 해킹, 시스템 침입, 시스템 관리자 권한 획득, 침입 사실 은닉, 서비스 거부공격 등과 같은 다양한 형태의 네트워크 공격으

로 인해 인터넷은 항상 해킹의 위험에 노출되어 인터넷에 대한 침해가 증가하고 있고, 공공기관과 사회기반시설 및 금융 기관은 피해 규모가 점점 증가하며 그 영향력이 크다.

<23> 이러한 인터넷 보안문제를 해결하기 위해 바이러스 백신, 방화벽, 통합 보안 관리, 침입탐지시스템 등의 네트워크 보안 기술이 필요함에 있다.

<24> 이에 따라, 인터넷의 핵심 요소인 라우터는 네트워크의 데이터 패킷흐름을 제어하고 적합한 목적지에 도달하는 최적의 길을 결정한다. 즉, 라우터의 오류 또는 라우터에 대한 공격에 의한 피해는 전체 네트워크에 대한 피해가 될 수 있다. 그리고, 라우터가 내부와 외부 네트워크 사이나 서로 다른 네트워크 사이에서 트래픽을 관리하는 장치이므로 라우터에 대한 보안이 반드시 필요하다. 이에, 라우터에 대한 접근 제어와 불법 네트워크 침입을 라우터에서 제어하는 보안 기술이 필요하다.

<25> 또한, 기존 네트워크 보안 방식은 단일 기능의 개별적 보안 시스템 위주로 구현되어 보안 시스템간의 상호 연동이 어려우며 정보 보호 인프라의 구축이 복잡하고 어렵다는 문제점이 있다.

<26> 한편, 네트워크 노드의 보안 엔진 관리와 관련하여 공개된 다른 종래 기술로는 2001년 10월 30일자 제 2001-0067074 호로 등록된 "통합보안관리 시스템"에 개시되어 있다.

<27> 이와 같이, 개시된 선행기술과 본원 발명과의 차이점에 대하여 상세하게 설명하면, "통합보안관리 시스템"은 네트워크 침입탐지를 관리하는 통합보안관리 시스템에 관한 것으로, 특히 다양한 침입탐지시스템으로부터 발생되는 이벤트 로그를 탐지유형 및 위험도에 따라 재분류한 매핑테이블을 이용해 매핑 이벤트 로그로 정규화하여 관리하는 통합보안관리시스템에 관한 것이다.

<28> 즉, 침입탐지시스템은 네트워크 환경에서 침입 또는 의심스러운 행위를 탐지하는 시스템으로서 탐지되는 패턴에 따라 위험도를 분류하여 탐지된 결과를 사용자에게 알려준다.

<29> 다양한 침입탐지시스템들의 침입탐지 패턴을 정형화된 매핑테이블로 구현하여 적재하고, 다양한 침입탐지시스템으로부터 발생되는 이벤트 로그를 매핑과정을 거쳐 정형화된 매핑 이벤트 로그로 변환하여 일관된 위험관리를 가능하게 하는 통합보안관리시스템을 제공한다.

<30> 그러나, 본원 발명과 종래 기술과의 차이점은 종래 기술은 다양한 종류의 침입탐지시스템들의 로그 분석과 일관된 위험 관리를 가능하게 하는데 중점을 둔 반면, 본원 발명은 침입탐지를 최적화하고 불법 네트워크 침입에 실시간으로 대응하고 관리하는 바와 같이 차이가 있다.

<31> 그리고, 종래 기술은 침입 탐지를 위한 침입탐지 패턴의 정형화에 중점을 둔 반면, 본원 발명은 침입의 탐지, 분석, 내부자의 침입을 방지하는 접근제어를 제공하며, 보안 정책에 의한 관리를 제공하는 바와 같이 상이하다.

<32> 마지막으로, 종래 기술은 다양한 침입탐지 패턴을 정형화하고 매핑 이벤트 로그를 이용하여 일관된 위험관리를 제공하는 통합관리시스템에 중점을 둔 반면, 본원 발명은 커널 영역에서 패킷 필터링과 침입 분석을 제공하여 침입 탐지를 최적화하며, 보안 정책에 의한 통합 보안 관리를 제공하는 바와 같이 차이가 있다.

<33> 이에 따라서, 정보 통신기술의 진화에 따라 새롭게 등장하는 보안 취약점에 따라 발생 가능한 여러 유형의 사이버 테러에 능동적으로 강력하게 대응 할 수 있는 통합 보안 네트워킹이 필요하게 되었다.

【발명이 이루고자 하는 기술적 과제】

<34> 이에, 본 발명은 상술한 통합 보안 네트워킹의 필요에 따라 안출된 것으로서, 그 목적은 네트워크 공격에 대응하는 보안 기능을 갖는 라우터나 게이트웨이 등의 네트워크 노드를 위해 커널 영역에서 패킷 필터링, 침입 분석 및 감사 추적, 인증 및 접근제어 관리의 보안 기능을 제공하여 침입 탐지를 최적화하고 불법 네트워크 침입에 실시간으로 대응하며, 보안 정책에 의해 네트워크 노드를 관리할 수 있도록 하는 네트워크 노드의 보안 엔진 관리 장치 및 방법을 제공함에 있다.

<35> 상술한 목적을 달성하기 위한 본 발명의 일실시 예에 따른 네트워크 노드의 보안 엔진 관리 장치는 시스템의 자원에 접근할 수 있는 모든 응용 프로그램과 유틸리티들을 처리하는 보안 명령어 및 라이브러리 서브시스템과, 네트워크로의 침입 탐지 및 차단에 필요한 필터링 정책, 침입 탐지 정책, 접근제어 정책을 결정하는 정책 결정 서브시스템과, 접근 제어 정책을 참조하여 허가받지 않은 사용자의 시스템 사용을 막고 모든 주체는 객체에 접근 할 수 있는 권한을 가진 경우에만 접근이 가능하도록 하는 인증 및 접근제어 서브시스템과, 정책들을 해석하여 정책을 적용하는 정책 적용 서브시스템과, 정책 적용에 따라 필터링 정책을 참조하면서 허가된 패킷은 수신하고, 허가되지 않은 패킷을 거부하는 패킷 필터링 서브시스템과, 정책 적용에 따라 침입탐지 정책을 참조하면서 네트워크의 침입을 분석하고 침입에 대응하는 침입 분석 및 감사 추적 서브시스템과, 보안 엔진을 관리하는 보안 관리 서브시스템을 포함하는 것을 특징으로 한다.

<36> 그리고, 상술한 목적을 달성하기 위한 본 발명의 다른 실시 예에 따른 네트워크 노드의 보안 엔진 관리 방법은 공격 시스템으로부터 제공되는 패킷을 수신하여 필터링 정책에 의해 검사하는 단계와, 검사 결과가 허가된 패킷인가를 판단하는 단계와, 판단에서 허가된 패킷일 경

우, 허가된 패킷을 통과시킨 후, 침입탐지 정책을 이용하여 검사한 결과가 공격 침입 패킷인가를 확인하는 단계와, 확인에서 공격 침입 패킷일 경우, 보안관리 GUI에 공격 침입 패킷임을 표시하며, 해당 패킷을 모두 거부하고, 이동 단말기에 단문 메시지 서비스로 공격 침입 패킷을 표시하는 단계를 포함하는 것을 특징으로 한다.

【발명의 구성 및 작용】

<37> 이하, 첨부된 도면을 참조하여 본 발명에 따른 실시 예를 상세하게 설명하기로 한다.

<38> 도 1은 본 발명의 바람직한 실시 예에 따른 공격 시스템(10-1)으로부터 침입을 차단하는 보안 엔진의 개괄적인 구성도를 도시한 도면이다. 도 1을 참조하면, 보안 네트워크(20)는 보안 엔진이 탑재된 라우터(100)와, 이동 단말기(S1)와 무선 통신하는 보안 관리 서브시스템(200)으로 구비된다.

<39> 즉, 공격 시스템(10-1)은 외부 네트워크에서 허브(S2-1)와 일반 라우터(S3-1)를 거쳐 보안 네트워크(20)와 일반 네트워크(30)에 공격을 시도한다.

<40> 그러면, 보안 네트워크(20)내 보안 엔진이 탑재된 라우터(100)는 필터링 정책과 침입 탐지 정책을 이용하여 네트워크 공격을 탐지하여 차단하고 이를 보안 관리 서브시스템(200)에 통지한다.

<41> 이후, 보안 관리 서브시스템(200)은 관리자의 이동 단말기(S1)로 침입이 발생했음을 단문메시지서비스(SMS)로 알린다.

<42> 이와 같이, 보안 엔진으로 구성된 보안 네트워크(20)는 침입을 차단할 수 있지만, 일반 네트워크(30)는 침입이 발생하면 공격을 당해 일반 라우터(S3-2)는 일반 시스템(10-2)으로 라우팅을 수행하지 못한다.

<43> 도 2는 도 1에 도시된 보안 네트워크 블록(20)의 상세 구성도로서, 도 2의 도면을 참조하면서 각 구성에 대해 상세하게 설명한다.

<44> 이중, 보안 엔진이 탑재된 라우터(100)는 보안 명령어 및 라이브러리 서브시스템(110)과, 정책 데이터베이스(120-1)에 연동된 정책 결정 서브시스템(120)과, 접근제어 정책(130-1)에 연동된 인증 및 접근제어 서브시스템(130)과, 정책 적용 서브시스템(140)과, 필터링 정책(150-1)에 연동된 패킷 필터링 서브시스템(150)과, 침입 탐지 정책(160-2) 및 감사 기록 데이터베이스(160-1)에 연동된 침입 분석 및 감사 추적 서브시스템(160)으로 구성되어 있다.

<45> 보안 명령어 및 라이브러리 서브시스템(110)은 인증 및 접근, 접근 속성 획득/변경을 인증 및 접근 제어 서브 시스템(130)에 요청하고, 그 결과를 제공받는 블록으로서, 시스템의 자원에 접근할 수 있는 모든 응용 프로그램과 유틸리티들을 처리한다. 그리고, 보안 명령어 및 라이브러리 서브시스템(110)은 정책 결정 서브시스템(120)으로부터 제공되는 접근 속성 요청에 대응하여 접근 속성을 제공한다.

<46> 정책 결정 서브시스템(120)은 침입 탐지 및 차단에 필요한 필터링 정책, 침입 탐지 정책, 접근제어 정책을 결정한 정책을 정책 적용 서브시스템(140)에 제공함과 동시에 정책을 정책 데이터베이스(120-1)에 저장한다.

<47> 인증 및 접근제어 서브시스템(130)은 보안 명령어 및 라이브러리 서브시스템(110)으로부터 요청된 인증 및 접근, 접근 속성 획득/변경에 대응하는 결과를 전달하며, 정책 적용 서브시스템(140)의 정책 적용에 응답하기 위해 접근 제어 정책(130-1)을 참조하여 허가받지 않은 사용자의 시스템 사용을 막고 모든 주체는 객체에 접근 할 수 있는 권한을 가진 경우에만 접근이 가능하도록 하고, 그 결과를 정책 적용 서브 시스템(140)에 제공한다.

<48> 즉, 인증 및 접근제어 서브시스템(130)은 보안 관리자만이 라우터의 라우팅 테이블 정보를 수정할 수 있기 때문에, 스니핑 프로그램으로 루트의 비밀번호를 알아낸 후 루트 권한을 획득하여 라우팅 테이블을 변경하려 해도 접근 권한을 가지는 보안 관리자가 아니므로 변경이 불가능하며 라우터 자체의 보안을 높일 수 있다.

<49> 정책 적용 서브시스템(140)은 정책 결정 서브시스템(120)으로부터 제공받은 정책들을 해석하여 인증 및 접근 제어 서브시스템(130) 및 패킷 필터링 서브시스템(150), 침입 분석 및 감사 서브시스템(160)에 정책을 적용한다.

<50> 그리고, 정책 적용 서브시스템(140)은 침입 분석 및 감사 추적 서브시스템(160)으로부터 제공받은 침입탐지 및 감사 정보를 디바이스 드라이버(S4)를 통해 정책 결정 서브시스템(120)에 제공하는 인터페이스 역할을 하며, 또한 패킷 필터링 서브시스템(150)으로부터 제공된 패킷 통계 정보를 proc 파일 시스템(S5)을 통해 정책 결정 서브시스템(120)에 제공한다.

<51> 패킷 필터링 서브시스템(150)은 정책 적용 서브시스템(140)의 정책 적용에 따라 필터링 정책(150-1)을 참조하여 필터링 정책(150-1)에 의해 허가된 패킷은 수신하고, 허가되지 않은 패킷을 거부하고, 그 결과를 정책 적용 서브시스템(140)에 제공한다. 여기서, 필터링 정책(150-1)은 발신지 주소, 목적지 주소, 발신지 포트, 목적지 포트, 프로토콜 종류에 따라 달라지는 것으로, 즉, 특정 목적지 주소의 패킷을 차단하거나 통과시키며, TCP, UDP, ICMP 등의 프로토콜에 해당하는 패킷을 차단하거나 통과시킨다.

<52> 침입 분석 및 감사 추적 서브시스템(160)은 정책 적용 서브시스템(140)의 정책 적용에 따라 침입탐지 정책(160-2)을 참조하여 침입탐지 정책(160-2)에 의해 네트워크의 침입을 분석하고 침입에 대응하고, 그 결과를 정책 적용 서브시스템(140)에 제공한다. 여기서, 침입탐지 정책(160-2)은 DoS 공격과 특정 바이러스 패턴을 탐지하는 규칙들로 구성된다. 특히, 웹 브라

우저를 통해 바이러스 파일을 다운로드 할 경우, 침입 분석 및 감사 추적 서브시스템(160)은 파일의 패턴을 검사하여 바이러스 파일 전송임을 탐지하고 정책 적용 서브시스템(140) 및 디바이스 드라이버(S4), 정책 결정 서브시스템(120)을 통해 보안 관리 서브시스템(200)내 웹 브라우저를 통해 시스템 관리자에게 알리며, 또한 공격 시스템(10-1)에서 DoS 공격을 시도할 경우, DoS 공격 패턴을 검사하여 DoS 공격을 차단하며, DoS 공격이나 바이러스 공격의 탐지 내용을 감사기록 데이터베이스(160-1)에 저장한다.

<53> 보안 관리 서브시스템(200)은 보안 엔진이 탑재된 라우터(100)를 통합 관리한다. 전체 네트워크 정보를 수집하여 네트워크 데이터베이스(208)에 저장하고, 저장된 네트워크 정보를 검색하여 네트워크를 관리하며, 도 3에 도시된 보안 관리 GUI(S6)를 이용하여 관리를 수행한다. 그리고, 이동 단말기(S1)를 사용하는 시스템 관리자에게 침입 탐지를 알려준다.

<54> 도 3은 도 2에 도시된 보안 관리 서브시스템(200)의 상세 구성도로서, 도 3의 도면을 참조하면서 각 구성에 대해 상세하게 설명한다.

<55> 보안 관리 서브시스템(200)은 로그인 처리 모듈(201)과, 패킷 통계 모듈(202)과, 네트워크 설정 모듈(203)과, 정책 관리 모듈(204)과, 감사 관리 모듈(205)과, XML Java Bean(206)과, 사용자 데이터베이스(207)와, 네트워크 데이터베이스(208)와, 네트워크 통신 모듈(209)로 구성되어 있다.

<56> 보다 상세하게 설명하면, 웹을 이용한 보안 관리 GUI(S6)을 통해 보안 관리 명령을 각각의 모듈(201, 202, 203, 204)들에 내리고, 각각의 모듈(201, 202, 203, 204)들은 보안 관리 GUI(S6)의 명령 요청에 응답하여 로그인을 처리하고, 패킷의 통계를 처리하며, 네트워크의 구성 현황을 지도로 보여주며 관리 도구를 보안 관리 GUI(S6)에 제공함과 동시에 정책의 추가, 삭제, 변경을 보안 관리 GUI(S6)에 제공한다.

<57> 그리고, 감사 관리 모듈(205)은 정책 결정 서브시스템(120)으로부터 네트워크 통신 모듈(209)을 통해 불법 침입에 대한 감사정보를 제공받아 처리하여 보안 관리 GUI(S6)에 제공한다.

<58> 보안 관리 GUI(S6)는 웹 브라우저를 실행하여 보안 관리 서브시스템(200)에 접속하는 사용자 인터페이스로서, 웹 브라우저에서 사용자 ID와 비밀번호를 입력할 경우, 로그인 처리 모듈(201)은 XML Java Bean(206)을 통해 사용자 데이터베이스(207)에 접근하여 읽기/쓰기를 통해 로그인 요청에 응답한다.

<59> 즉, 사용자 데이터베이스(207)에 있는 데이터를 참고하여 로그인을 허가하거나 차단한다. 여기서, 관리 명령을 왼쪽 트리 메뉴에서 실행이 가능하며, 오른쪽 버튼을 누르면 나타나는 팝업 메뉴에서도 실행이 가능하다.

<60> 패킷 통계 모듈(202) 및 네트워크 설정 모듈(203)은 네트워크 데이터베이스(208)에 있는 데이터를 이용하여 프로토콜과 인터페이스 별로 패킷 통계정보로 보여주고, 라우터와 시스템들의 네트워크 상황을 지도로 구성하여 보안 관리 GUI(S6)를 통해 보여준다.

<61> 이중, 네트워크 설정 모듈(203)은 인터페이스 카드 종류, IP 주소, 하드웨어 주소, MTU 크기, 상태 및 옵션의 네트워크 인터페이스 정보와 OS 정보, 부팅 경과 시간, 현재 시간, 시스템 이름, 디스크 크기의 시스템 정보를 보여주고, 라우팅 테이블의 추가, 삭제 및 수정을 할 수 있다.

<62> 다음으로, 정책 관리 모듈(204)은 네트워크 침입 탐지를 위한 보안 정책을 보여주고, 추가, 삭제, 편집을 수행한다. 즉, 침입 패킷의 자동 폐기 기능이 있어 오프(Off) 상태에서는 침입이 발생하면 탐지만 하고, 온(On) 상태에서는 침입이 탐지되면 보안 관리자에게 단문메시지 서비스(SMS)로 알려주고 패킷을 자동으로 폐기한다.

<63> 감사 관리 모듈(205)은 라우터가 DoS공격이나 바이러스 공격을 받으면 공격내용을 보안 관리 GUI(S6)에 실시간으로 표시하고 단문메시지서비스(SMS)를 이용하여 관리자에게 알려준다.

<64> 네트워크 통신 모듈(209)은 정책 관리를 위해 정책결정 서브시스템(120)과의 통신을 처리하고, 감사 모듈로의 실시간 통지를 처리한다.

<65> 도 4의 흐름도를 참조하면, 상술한 구성을 바탕으로, 본 발명에 따른 공격 시스템(10-1)의 침입을 탐지하고 실시간으로 대응하는 보안 엔진(100)의 동작 과정에 대하여 상세하게 설명한다.

<66> 먼저, 보안 엔진이 탑재된 라우터(100)는 공격 시스템(10-1)으로부터 허브(S2-1) 및 일반 라우터(S3-1)를 통해 제공되는 패킷을 수신하여 필터링 정책에 의해 검사한다(단계 401).

<67> 즉, 검사 과정에서 필터링 정책으로 검사한 결과가 허가된 패킷인가를 판단한다(단계 402).

<68> 상기 판단 단계(402)에서 허가되지 않은 패킷일 경우, 패킷을 거부한다(단계 403).

<69> 반면에, 상기 판단 단계(402)에서 허가된 패킷일 경우, 허가된 패킷을 통과시킨 후, 침입탐지 정책을 이용하여 검사한 결과가 공격 침입 패킷인가를 확인한다(단계 404).

<70> 상기 확인 단계(404)에서 공격 침입 패킷일 경우, 보안관리 GUI(S6)에 공격 침입 패킷임을 표시하며, 문자 해당 패킷을 모두 거부하고(단계 405), 이동 단말기(S1)에 단문 메시지 서비스로 공격 침입 패킷을 표시한다(단계 406).

<71> 반면에, 상기 확인 단계(404)에서 공격 침입 패킷이 아닌 일반 패킷일 경우, 해당 네트워크를 통해 패킷을 전달한다(단계 407).

<72> 도 5의 흐름도를 참조하면, 상술한 구성을 바탕으로, 본 발명에 따른 보안 엔진이 탑재된 라우터(100)와 보안 관리 서브시스템(200)간의 보안 정책에 의해 통합적으로 보안 관리를 제공하는 과정에 대하여 보다 상세하게 설명한다.

<73> 먼저, 사용자 등록 및 인증 과정을 통해 허가되지 않은 사용자의 접속을 통제 여부를 판단한다(단계 501).

<74> 상기 판단 단계(501)에서 허가된 사용자일 경우, 보안관리 서브시스템(200)에 접속한다(단계 502).

<75> 네트워크 노드의 중요한 자원을 허가받지 않은 사용자들이 접근하는 것을 차단하며, 불법으로 루트 권한을 획득하여 발생하는 피해를 차단한다(단계 504).

<76> 그리고, 보안 정책에 기반하여 보안 엔진을 관리하며, 보안 정책을 정책 데이터베이스(120-1)에 저장한다(단계 505).

<77> 보안 관리 서브 시스템(200)은 호스트, 게이트웨이, 라우터들의 네트워크 구성을 나타내기 위해 정보를 수집하며, 수집된 정보를 네트워크 데이터베이스(208)에 저장한다(단계 506).

<78> 이후, 보안 관리 서브 시스템(200)은 사용자 인터페이스인 보안 관리 GUI(S6)에 연동된 웹 브라우저로 보안 관리 내용을 표시하도록 제어한다(단계 507).

<79> 상기 판단 단계(501)에서 허가된 사용자가 아닐 경우, 보안관리 서브시스템(200)에 접속이 되지 않도록 차단한다(단계 503).

<80> 또한, 이상과 같이 도 4 내지 도 5를 참조하여 기술된 본 발명에 따른 네트워크 노드의 보안 엔진 관리 장치 및 방법은 이에 대응하는 프로그램으로 구현되어 기록 매체로 저장될 수

있으며, 기록 매체에 저장된 프로그램은 본 발명의 장치에 대응하는 하드웨어 또는 범용 하드웨어에서 실행될 수 있다.

【발명의 효과】

<81> 상기와 같이 설명한 본 발명은 네트워크 공격에 대응하는 보안 기능을 갖는 라우터나 게이트웨이 등의 네트워크 노드를 위해 커널 영역에서 패킷 필터링, 침입 분석 및 감사 추적, 인증 및 접근제어 관리의 보안 기능을 제공하여 침입 탐지를 최적화하고 불법 네트워크 침입에 실시간으로 대응하며, 보안 정책에 의해 네트워크 노드를 관리함으로써, 보안 환경의 변화에 민첩하게 대처할 수 있다. 또한, 기존 네트워크 노드들의 자체 보안 결함을 해결하며 통합적인 보안 관리를 제공하고, 웹 브라우저를 사용하여 관리의 편리성과 효율성을 제공하는 효과가 있다.

【특허청구범위】

【청구항 1】

네트워크 노드의 보안 엔진 관리 장치에 있어서,

시스템의 자원에 접근할 수 있는 모든 응용 프로그램과 유틸리티들을 처리하는 보안 명령어 및 라이브러리 서브시스템과,

상기 네트워크로의 침입 탐지 및 차단에 필요한 필터링 정책, 침입 탐지 정책, 접근제어 정책을 결정하는 정책 결정 서브시스템과,

상기 정책 적용에 응답하기 위해 접근 제어 정책을 참조하여 허가받지 않은 사용자의 시스템 사용을 막고 모든 주체는 객체에 접근 할 수 있는 권한을 가진 경우에만 접근이 가능하도록 하는 인증 및 접근제어 서브시스템과,

상기 정책들을 해석하여 정책을 적용하는 정책 적용 서브시스템과,

상기 정책 적용에 따라 필터링 정책을 참조하면서 허가된 패킷은 수신하고, 허가되지 않은 패킷을 거부하는 패킷 필터링 서브시스템과,

상기 정책 적용에 따라 침입탐지 정책을 참조하면서 네트워크의 침입을 분석하고 침입에 대응하는 침입 분석 및 감사 추적 서브시스템과,

상기 보안 엔진을 관리하는 보안 관리 서브시스템

을 포함하는 것을 특징으로 하는 네트워크 노드의 보안 엔진 관리 장치.

【청구항 2】

제 1 항에 있어서,

상기 정책 적용 서브시스템은, 침입탐지 및 감사 정보에 대하여 디바이스 드라이버를 통해 제공하며, 패킷 통계 정보에 대하여 proc 파일 시스템을 통해 제공하는 것을 특징으로 하는 네트워크 노드의 보안 엔진 관리 장치.

【청구항 3】

제 1 항에 있어서,

상기 필터링 정책은, 발신지 주소, 목적지 주소, 발신지 포트, 목적지 포트, 프로토콜 종류에 따라 특정 목적지 주소의 패킷을 차단 및 통과시키며, TCP, UDP, ICMP 등의 프로토콜에 해당하는 패킷을 차단 및 통과시키는 것을 특징으로 하는 네트워크 노드의 보안 엔진 관리 장치.

【청구항 4】

제 1 항에 있어서,

상기 침입탐지 정책은, DoS 공격과 특정 바이러스 패턴을 탐지하는 규칙들로 구성되어 있는 것을 특징으로 하는 네트워크 노드의 보안 엔진 관리 장치.

【청구항 5】

제 1 항에 있어서,

상기 침입 분석 및 감사 추적 서브시스템은, 상기 바이러스 파일이 다운로드 될 경우, 파일 패턴을 검사하여 바이러스 파일 전송임을 탐지하여 이동 단말기에 송출하며, DoS 공격이 시도될 경우, DoS 공격 패턴을 검사하여 DoS 공격을 차단하며, DoS 공격이나 바이러스 공격의 탐지 내용을 감사기록 데이터베이스에 저장하는 것을 특징으로 하는 네트워크 노드의 보안 엔진 관리 장치.

【청구항 6】

제 1 항에 있어서,

상기 보안 관리 서브시스템은,

관리 명령을 수행하는 사용자 인터페이스로 웹을 이용한 보안 관리 GUI와,

불법 침입에 대한 감사정보를 처리하는 감사 관리 모듈과,

상기 이동 단말기에서 사용자 ID와 비밀번호가 입력될 경우, 상기 사용자 ID와 비밀번호를 처리하여 사용자의 인증을 담당하는 로그인 처리 모듈과,

프로토콜과 인터페이스 별로 패킷 통계정보로 보여주는 패킷 통계 모듈과,

라우터와 시스템들의 네트워크 상황을 지도로 구성하여 상기 보안 관리 GUI를 통해 보여주는 네트워크 설정 모듈과,

네트워크 침입 탐지를 위한 보안 정책을 보여주고, 추가, 삭제, 편집을 수행하는 정책 관리 모듈과,

DoS 공격 및 바이러스 공격 내용을 표시하고 상기 공격 내용을 단문메시지서비스를 이용하여 상기 이동 단말기에 알려주는 감사 관리 모듈과,

정책 관리를 위해 상기 정책결정 서브시스템과의 통신을 처리하고, 감사 모듈로의 실시간 통지를 처리하는 네트워크 통신 모듈

을 더 포함하는 것을 특징으로 하는 네트워크 노드의 보안 엔진 관리 장치.

【청구항 7】

제 6 항에 있어서,

상기 네트워크 설정 모듈은, 인터페이스 카드 종류, IP 주소, 하드웨어 주소, MTU 크기, 상태 및 옵션의 네트워크 인터페이스 정보와 OS 정보, 부팅 경과 시간, 현재 시간, 시스템 이름, 디스크 크기의 시스템 정보를 보여주고, 라우팅 테이블의 추가, 삭제 및 수정하는 것을 특징으로 하는 네트워크 노드의 보안 엔진 관리 장치.

【청구항 8】

제 6 항에 있어서,

상기 정책 관리 모듈은, 침입 패킷의 자동 폐기 기능이 있어 오프(Off) 상태에서 침입이 발생될 경우 탐지만 하며, 온(On) 상태에서 침입이 탐지될 경우, 상기 이동 단말기에 단문메시지서비스로 알려주고 패킷을 자동 폐기하는 것을 특징으로 하는 네트워크 노드의 보안 엔진 관리 장치.

【청구항 9】

네트워크 노드의 보안 엔진 관리 방법에 있어서,

공격 시스템으로부터 제공되는 패킷을 수신하여 필터링 정책에 의해 검사하는 단계와,

상기 검사 결과에서 허가된 패킷인가를 판단하는 단계와,

상기 판단에서 허가된 패킷일 경우, 허가된 패킷을 통과시킨 후, 침입탐지 정책을 이용하여 검사한 결과가 공격 침입 패킷인가를 확인하는 단계와,

상기 확인에서 공격 침입 패킷일 경우, 보안관리 GUI에 공격 침입 패킷임을 표시하고, 이동 단말기에 단문 메시지 서비스로 공격 침입 패킷을 표시하며, 해당 패킷을 모두 거부하는 단계

를 포함하는 것을 특징으로 하는 네트워크 노드의 보안 엔진 관리 방법.

【청구항 10】

제 9 항에 있어서,

상기 판단에서 허가되지 않은 패킷일 경우, 패킷을 거부하는 것을 특징으로 하는 네트워크 노드의 보안 엔진 관리 방법.

【청구항 11】

제 9 항에 있어서,

상기 확인 단계에서 공격 침입 패킷이 아닌 일반 패킷일 경우, 해당 네트워크를 통해 패킷을 전달하는 것을 특징으로 하는 네트워크 노드의 보안 엔진 관리 방법.

【청구항 12】

라우터와 보안 관리 서브시스템간의 보안 정책에 의해 통합적으로 보안 관리를 제공하는 방법에 있어서,

사용자 등록 및 인증 과정을 통해 허가되지 않은 사용자의 접속을 통제 여부를 판단하는 단계와,

상기 판단에서 허가된 사용자일 경우, 보안관리 서브시스템에 접속하여 호스트, 게이트웨이, 라우터들의 네트워크 구성을 나타내기 위해 정보를 수집하며, 상기 수집된 정보를 네트워크 데이터베이스에 저장하는 단계와,

사용자 인터페이스인 보안 관리 GUI로 보안 관리 내용을 표시하는 단계

를 포함하는 것을 특징으로 하는 네트워크 노드의 보안 엔진 관리 방법.

【청구항 13】

제 12 항에 있어서,

상기 판단 단계에서 허가된 사용자가 아닐 경우, 보안관리 서브시스템에 접속되지 않도록 함과 동시에 네트워크 노드의 중요한 자원을 허가받지 않은 사용자들이 접근하는 것을 차단하며, 불법으로 루트 권한을 획득하여 발생하는 피해를 차단하는 것을 특징으로 하는 네트워크 노드의 보안 엔진 관리 방법.

【청구항 14】

제 13 항에 있어서,

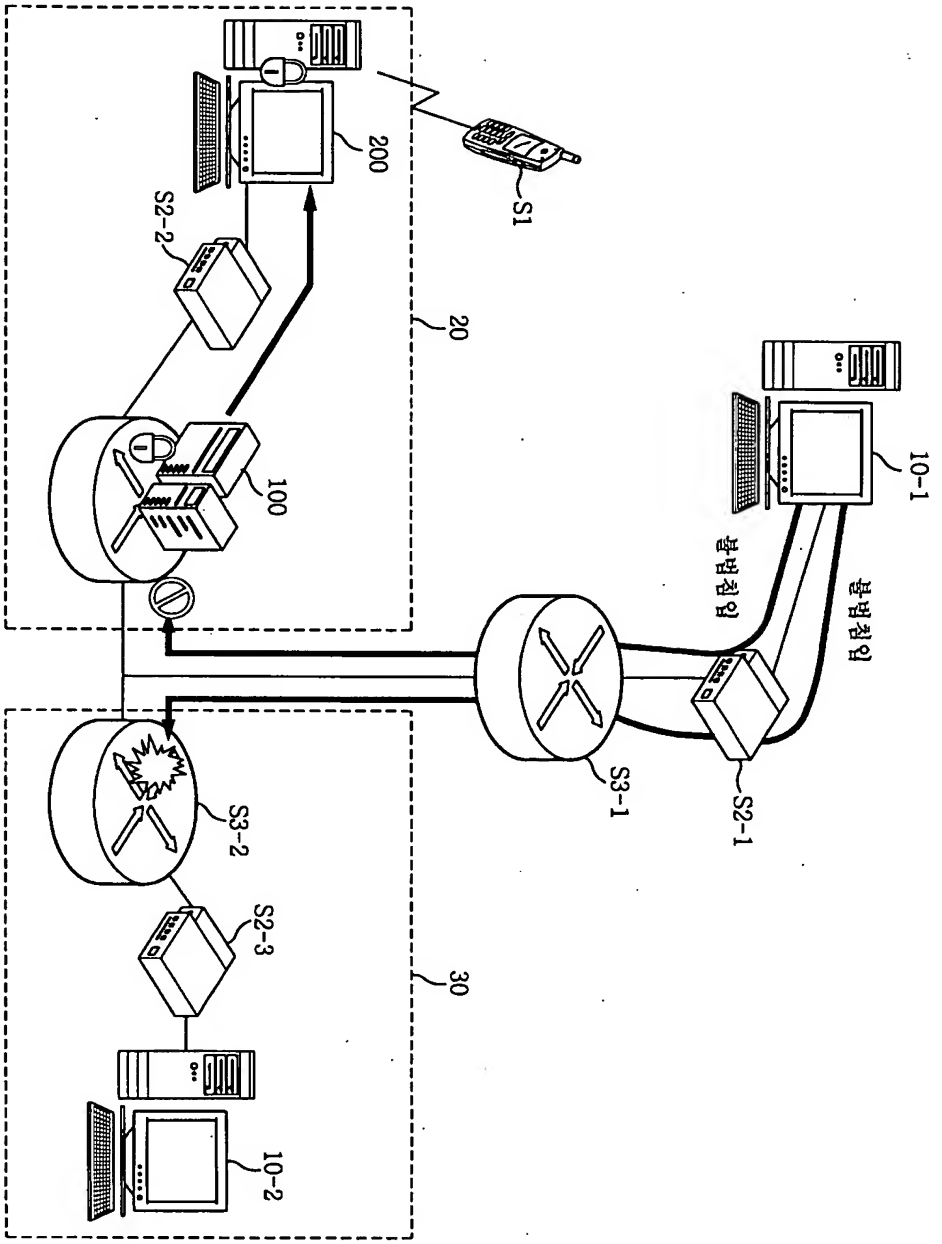
상기 판단 단계에서 허가된 사용자가 아닐 경우, 보안 정책에 기반하여 보안 엔진을 관리하며, 보안 정책을 정책 데이터베이스에 저장하는 것을 특징으로 하는 네트워크 노드의 보안 엔진 관리 방법.

【청구항 15】

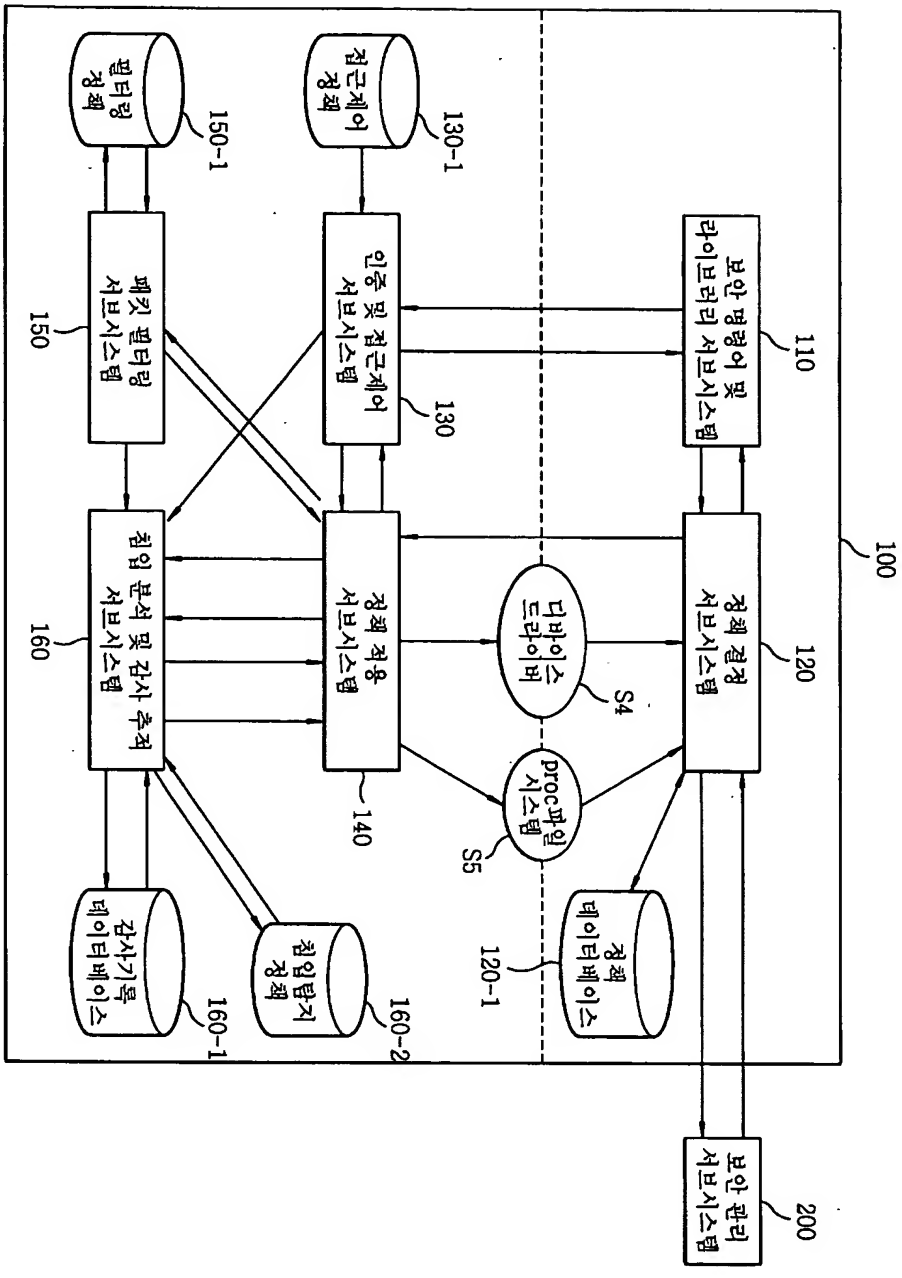
제 9 항 내지 제 14 항의 방법 중의 하나를 구현하는 프로그램을 기록한 기록 매체.

【도면】

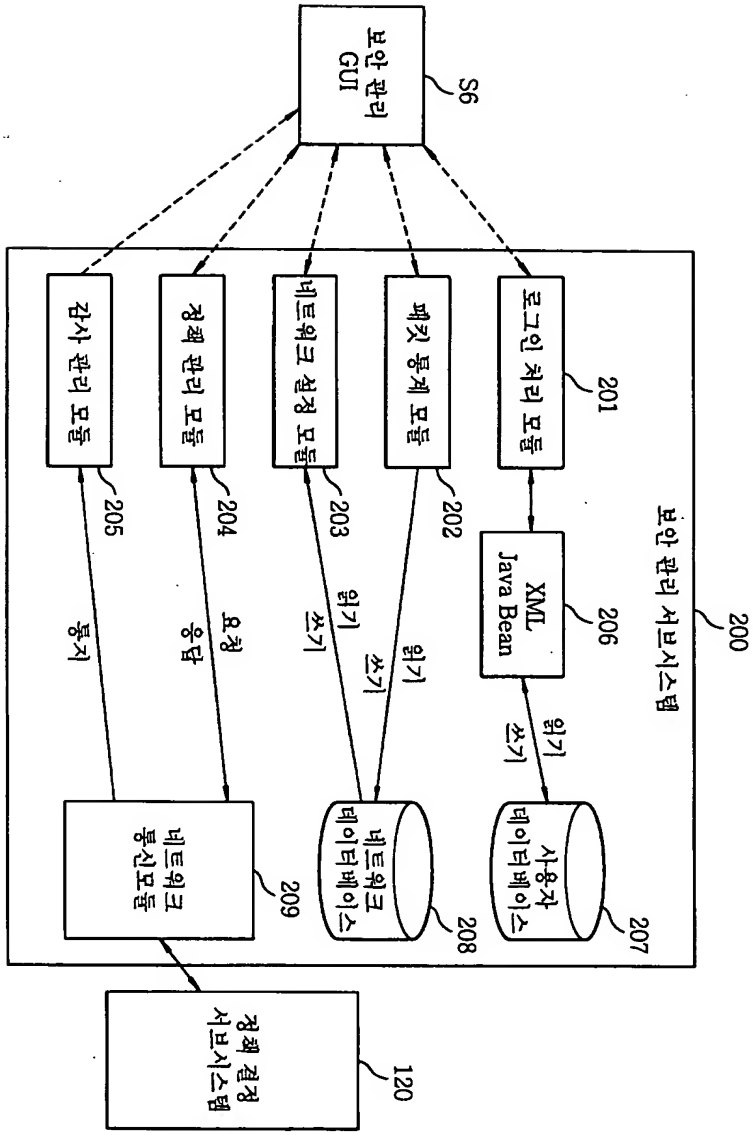
【도 1】



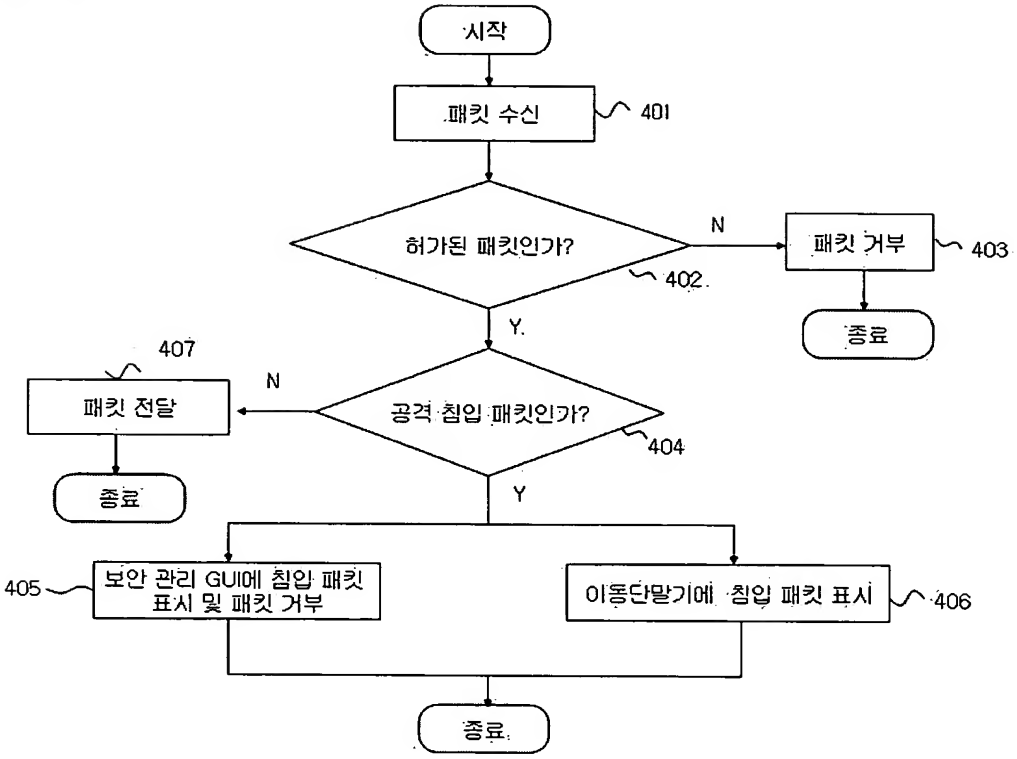
【도 2】


보안 명령어 및 라이브러리 서브시스템
110
정책 결정 서브시스템
120
보안 관리 서브시스템
200
인증 및 접근제어 서브시스템
130
정책 적용 서브시스템
140
패킷 필터링 서브시스템
150
침입 분석 및 감사 추적 서브시스템
160
디바이스 드라이버
S4
proc파일 시스템
S5
100
접근제어 정책
130-1
필터링 정책
150-1
정책 데이터베이스
120-1
감사기록 데이터베이스
160-1
침입탐지 정책
160-2

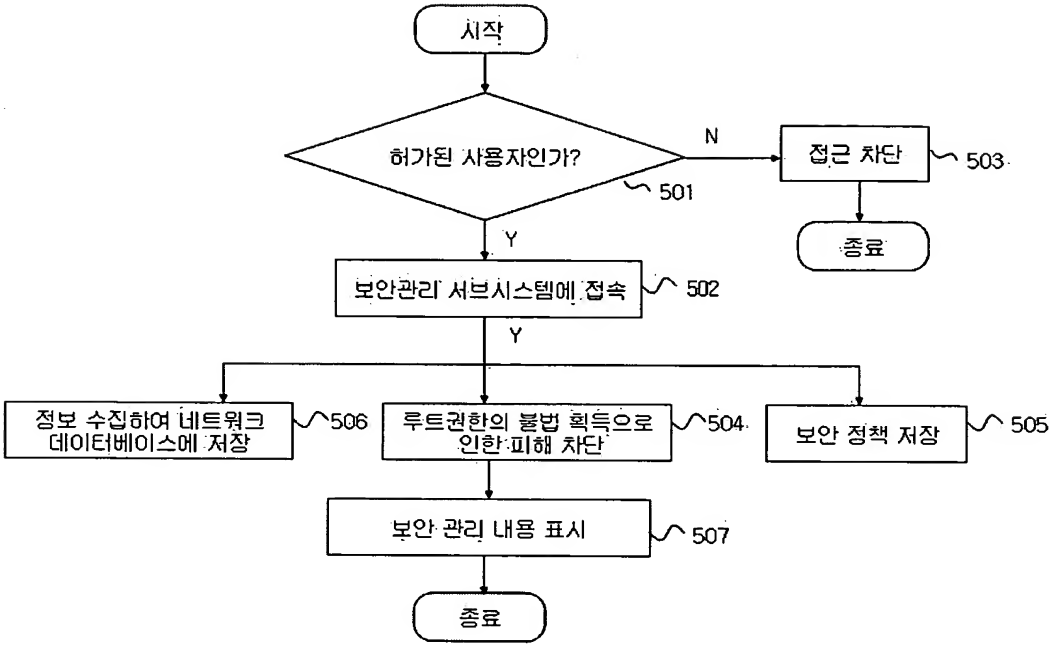
【도 3】


보안 관리 GUI
S6
보안 관리 서브시스템
200
로그인 처리 모듈
201
패킷 통계 모듈
202
네트워크 설정 모듈
203
정책 관리 모듈
204
감사 관리 모듈
205
XML Java Bean
206
사용자 데이터베이스
207
네트워크 데이터베이스
208
네트워크 통신모듈
209
정책 결정 서브시스템
120
읽기
쓰기
읽기
쓰기
요청
응답
통지

【도 4】


시작
패킷 수신
401
허가된 패킷인가?
402
N
패킷 거부
403
종료
Y
407
패킷 전달
N
공격 침입 패킷인가?
404
종료
Y
405
보안 관리 GUI에 침입 패킷 표시 및 패킷 거부
이동단말기에 침입 패킷 표시
406
종료

【도 5】


시작
허가된 사용자인가?
501
N
접근 차단
503
종료
Y
보안관리 서브시스템에 접속
502
Y
정보 수집하여 네트워크 데이터베이스에 저장
506
루트권한의 불법 획득으로 인한 피해 차단
504
보안 정책 저장
505
보안 관리 내용 표시
507
종료